North Shore-LIJ Health System is now **Northwell Health**

POLICY TITLE: Media Reuse and Disposal Policy	**ADMINISTRATIVE POLICY AND PROCEDURE MANUAL**
POLICY #: 900.26	**CATEGORY:** Information Services
System Approval Date: 4/20/17 **Site Implementation Date:** 5/23/17	**Effective Date:** 10/25/12 **Last Reviewed/Approved:** 12/13/12
Prepared by: Office of the CIO - IS Policy & Procedure Committee	**Superseded Policy(s)/#/Notations:** 900.29 Equipment Disposal Policy *Previously Titled: Device and Media Control Policy*

GENERAL STATEMENT of PURPOSE

This purpose of this policy is to provide procedures and guidelines that address the receiving, removal, re-use, and disposal (including data backup upon disposal or re-use) of hardware and electronic media containing sensitive or highly sensitive information such as protected health information (PHI), card holder data, and personally identifiable information (PII) to minimize the risk of the inadvertent disclosure of this information. This policy applies to all hardware and electronic media, including but not limited to: computers, mobile devices, network infrastructure hardware, backup media, telecommunication equipment, medical devices, and storage devices.

POLICY

It is the policy of Northwell Health, ("Northwell") to lawfully and efficiently secure and maintain the confidentiality of all sensitive and highly sensitive information during receiving, removal, re-use, and disposal of hardware and electronic media.

SCOPE

This policy applies to all Northwell Health employees, as well as medical staff, volunteers, students, trainees, physician office staff, contractors, trustees and other persons performing work for or at Northwell Health; faculty and students of the Hofstra Northwell School of Medicine conducting research on behalf of the School of Medicine on or at any Northwell Health facility; and the faculty and students of the Hofstra Northwell School of Graduate Nursing and Physician Assistant Studies.

DEFINITIONS

Business Unit Leadership: The managers and directors within the various hospitals, physicians' offices, and other facilities, departments, and programs that make up Northwell.

Computing Device (Hardware): An electronic device for processing information and performing calculations such as computers, laptops, and servers (and all internal components), keyboards, monitors, hard disk drives (both fixed and removable), smartphones, and tablets.

Disposal/Sanitation Vendor: A third party vendor engaged by Northwell to collect and physically destroy or sanitize computing devices and electronic media in accordance with Northwell standards.

Hardware and Electronic Media: All stationary and portable hardware, devices, and storage that access or contain sensitive or highly sensitive information from Northwell's network. This includes, but is not limited to:

- Servers, workstations, and laptops
- Hard disk drives (fixed or removable)
- Implantable and wearable devices
- Smartphones and tablets
- mp3 players (in data mode)
- USB portable drives (for example, flash drives)
- SD cards and other removable memory cards
- CDs and DVDs

Highly Sensitive Information: Protected health information or any information that, if lost, corrupted, disclosed to or accessed by an unauthorized person, or disclosed or accessed by unauthorized means, may (i) violate federal, state, and/or local law, (ii) cause significant harm, injury or damage to another person or entity, or (iii) cause financial loss to another person or entity. Examples include, but are not limited to Social Security numbers, credit card data, and driver's license information. Refer to the *900.12 Data Classification and Handling Policy*.

Mobile Device: A small portable device, including tablets and smartphones, used for computing and/or communication.

Personally Identifiable Information (PII): Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

The following list contains examples of information that may be considered PII.

1. Name, such as full name, maiden name, mother's maiden name, or alias.
2. Personal identification number, such as Social Security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number.

3. Address information, such as street address or email address.
4. Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people.
5. Telephone numbers, including mobile, business, and personal numbers.
6. Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry).
7. Information identifying personally owned property, such as vehicle registration number or title number and related information.
8. Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

All PII shall at all times be subject to all applicable laws, including, without limitation, the New York State Social Security Number Protection Law, New York State Labor Law, and Fair Credit Reporting Act. This includes all PII relating to members of the Northwell workforce. All PII that is also PHI shall, at all times, also be subject to all applicable laws and Northwell policies regarding PHI, as set out above.

Protected Health Information (PHI): Any oral, written, or electronic individually identifiable health information. PHI may relate to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the payment for the provision of health care to an individual. The Health Insurance Portability and Accountability Act (HIPAA) further defines PHI as information that identifies the individual by one or more (depending on context) of the following 18 identifiers:

1. Names
2. Geographic subdivisions smaller than a state, including street address, city, county, precinct, Zip code, and their equivalent geocodes except for the initial three digits of a Zip code in certain situations
3. All elements of a date (except the year) directly related to an individual, including birth date, discharge date, date of death; and all ages over 89 and all elements of dates indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers
13. Medical device identifiers

14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) addresses
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code

Sensitive Information: Any information that, if lost, corrupted, disclosed to or accessed by an unauthorized person, or disclosed or accessed by unauthorized means, may cause harm, injury or damage to another person or entity. Examples include, but are not limited to a number of Personally Identifiable Information data elements that are not highly sensitive. Refer to the *900.12 Data Classification and Handling Policy*.

Workforce Members: All entities covered in the Scope section above.

PROCEDURE/GUIDELINES

1. **Data Destruction**
   Northwell sensitive and highly sensitive data that is no longer needed must be removed from computing devices or electronic media prior to re-use or disposal by:
   a. Physical destruction of the hardware or electronic media such that data is irretrievable; or
   b. Sanitization using methodologies consistent with the National Institute of Standards and Technology (NIST) publication 800-88 *Guidelines for Media Sanitization*.
2. **Disposal**
   The following procedures must be followed when electronic media or computing devices are no longer needed, have become nonfunctional or obsolete, or are otherwise ready to be destroyed or removed:
   a. Electronic media and computing hardware must be disposed of using methodologies consistent with the National Institute of Standards and Technology (NIST) publication 800-88 *Guidelines for Media Sanitization*.
   b. Computing devices or electronic media that is nonfunctioning must be physically destroyed before it is disposed of.
   c. For enterprise storage, hardware and other types of electronic media managed by Information Services containing confidential information (such as computer hard drives, removable storage devices, RAM modules, backup tapes, etc.), the device owner must make arrangements with either the IS Service Desk, disposal vendor, equipment manufacturer or leasor to have the computing hardware or electronic media properly disposed of.
   d. For personal electronic media (such as USB drives, thumb drives, CDs, etc.), personal computing devices (such as laptops, mobile phones, tablets, etc.), or department computing devices not managed by Information Services (such as servers, local storage devices, etc.) containing confidential information, the device owner must open an IS Service Desk ticket to have the electronic media or computing device properly disposed.
   e. Information Services will take possession of the computing device or electronic media, store it in a secured location, and make arrangements for its secure disposal.

f. Northwell must obtain a record of disposal including sanitization or destruction methods used (e.g., certificate of destruction) for all hardware and electronic media where sensitive or highly sensitive information is stored.

3. **Electronic Media or Computing Device Re-Use**
   The following guidelines must be followed when computing devices (hardware) or electronic media is repurposed for future use:
   a. Before the computing device or electronic media is sanitized and repurposed, the data must be backed up and securely stored in compliance with Northwell's data retention policy *(100.97 Records Retention and Destruction Policy).*
   b. For enterprise storage, computing hardware and other types of electronic media managed by Information Services containing confidential information, the device owner must make arrangements with the sanitation vendor, equipment manufacturer or leaser to have the computing device or electronic media properly sanitized prior to re-use.
   c. For personal electronic media (such as USB drives, thumb drives, CDs, etc.), personal computing devices (such as laptops, mobile phones or tablets etc.), or departmental managed computing devices not managed by Information Services (such as servers, local storage devices, etc.) containing confidential information, the device owner must open an IS Service Desk ticket to have the electronic media or computing device properly sanitized. Information Services will take possession of the computing device or electronic media, store it in a secured location and make arrangements to have it sanitized and returned to the device owner, as appropriate.
   d. Electronic media and computing devices that have been properly sanitized may be sold, recycled, reused, or returned (if leased).
   e. Northwell must retain a record of sanitization (e.g., IS Service Desk ticket) for computing devices.

4. **Disposal/Sanitation Vendor**
   a. The disposal/sanitation vendor must sanitize all confidential data from, or physically destroy, computing devices or electronic media using methodologies consistent with the National Institute of Standards and Technology (NIST) publication 800-88 *Guidelines for Media Sanitization*.
   b. Before contracting with a third party disposal vendor, Information Security must review the vendor to ensure physical security controls are implemented and destruction methods meet the requirements of this policy.
   c. The disposal/sanitation vendor must provide an inventory of all computing devices and electronic media sanitized or disposed of.

ENFORCEMENT

Users should report any violations of this policy immediately to their respective managers. If appropriate, the violation should be escalated and reported to the IS Service Desk or the Office of Corporate Compliance HelpLine. Anyone found in violation of this policy may be subject to disciplinary action, up to and including termination of employment or engagement, as applicable, in consultation with Human Resources.

CONTACT INFORMATION

What	Where
Northwell Health Service Desk	(516) (718) (631) 470-7272
Northwell Health Service Desk Email	servicedesk@northwell.edu
IT Security Hotline Email	ITSecurity@northwell.edu
Office of Corporate Compliance HelpLine	(800) 894-3226
Office of Corporate Compliance Website	www.northwell.ethicspoint.com

REFERENCES to REGULATIONS and/or OTHER RELATED POLICIES

- #100.009 Payment Card Industry Data Security Standards PCI DSS IT Security Policy
- #100.97 Records Retention and Destruction
- #800.02 Release of Protected Health Information for Living Patients Policy
- #800.47 Disposal Policy for Protected Health and Confidential Health System Information
- #900.12 Data Classification and Handling Policy
- *Health Information Technology for Economic and Clinical Health (HITECH) Act*
- Health Information Trust Alliance (HITRUST) Common Security Framework (CSF) Control Objective Name: 9.07 Media Handling
- *Health Insurance Portability and Accountability Act (HIPAA), Security Final Rule,* 45 CFR 164.310(d)(1) Device and Media Control – Disposal; Media Re-Use

CLINICAL REFERENCES/PROFESSIONAL SOCIETY GUIDELINES

N/A

ATTACHMENTS

N/A

FORMS

N/A

APPROVAL:	
System Administrative P&P Committee	3/30/17
System PICG/Clinical Operations Committee	4/20/17

Standardized Versioning History:

*=Policy Committee Approval; ** =PICG/Clinical Operations Committee Approval

*10/25/12 Provisional Approval

*11/29/12 Final Approval 12/13/12**